

**CLAIMS**

1. A method in a computer system for detecting intrusions, the method comprising:
  - 5 receiving a behavior profile associated with an application;  
reading the behavior profile associated with the application;  
monitoring execution of the application, according to the behavior profile;  
if the behavior of the application does not conform to the behavior profile,  
issuing a message indicating that the application is not conforming to the behavior  
10 profile.
2. The method of claim 1, where the application comprises any one of:
  - a software program running on a computer system;
  - a computer network;
  - 15 a user interfacing with a computer system;
  - a plurality of computer systems; and
  - a distributed application.
3. The method of claim 1, wherein the behavior profile is generated by at least  
20 one of:
  - a developer of the method;
  - a developer of the application; and
  - a third party developer.

**EXPRESS MAIL LABEL NO.: EV343426261US**

4. The method of claim 2, wherein the behavior profile is generated by any one of:

executing the system on a reference computer system;

heuristic determination; and

5 a combination of executing the system on a reference computer system and heuristic determination.

5. The method of claim 1, wherein the behavior profile includes at least one of:

a list of system commands;

10 a list of file permissions;

a list of directory permissions;

a list of network messages;

a login attempt summary; and

any measurable property of the system or application.

15

6. The method of claim 1, wherein the behavior profile is cryptographically protected.

7. The method of claim 6, wherein the behavior profile is at least one of:

20 encrypted; and

digitally signed.

**EXPRESS MAIL LABEL NO.: EV343426261US**

8. The method of claim 1, further comprising:

if the behavior of the application does not conform to the behavior profile, generating a log file describing how the application is not conforming to the behavior profile.

5

9. The method of claim 1, further comprising:

if the behavior of the application does not conform to the behavior profile, quitting the application that is not conforming to the behavior profile.

10 10. The method of claim 1, further comprising:

if the behavior of the application does not conform to the behavior profile, prompting the user to determine whether to quit the application that is not conforming to the behavior profile.

15

**EXPRESS MAIL LABEL NO.: EV343426261US**

11. A computer readable medium including computer instructions for detecting intrusions, the computer instructions including instructions for:

receiving a behavior profile associated with an application;

reading the behavior profile associated with the application;

5 monitoring execution of the application, according to the behavior profile; and  
if the behavior of the application does not conform to the behavior profile,  
issuing a message indicating that the application is not conforming to the behavior  
profile.

10 12. The computer readable medium claim 11, where the application comprises  
any one of:

a software program running on a computer system;

a computer network;

a user interfacing with a computer system;

15 a plurality of computer systems; and

a distributed application.

13. The computer readable medium of claim 12, wherein the behavior profile is  
generated by at least one of:

20 a developer of the method;

a developer of the application; and

a third party developer.

**EXPRESS MAIL LABEL NO.: EV343426261US**

14. The computer readable medium of claim 11, wherein the behavior profile is generated by any one of:

executing the system on a reference computer system;

heuristic determination; and

5 a combination of executing the system on a reference computer system and heuristic determination.

15. The computer readable medium of claim 11, wherein the behavior profile includes at least one of:

10 a list of system commands;

a list of file permissions;

a list of directory permissions;

a list of network messages;

a login attempt summary; and

15 any measurable property of the system or application.

16. The computer readable medium of claim 11, wherein the behavior profile is cryptographically protected.

20

**EXPRESS MAIL LABEL NO.: EV343426261US**

17. The computer readable medium of claim 16, wherein the behavior profile is at least one of:

encrypted; and

digitally signed.

5

18. The computer readable medium of claim 11, further comprising:

if the behavior of the application does not conform to the behavior profile, generating a log file describing how the application is not conforming to the behavior profile.

10

19. The computer readable medium of claim 11, further comprising:

if the behavior of the application does not conform to the behavior profile, quitting the application that is not conforming to the behavior profile.

15 20. The computer readable medium of claim 11, further comprising:

if the behavior of the application does not conform to the behavior profile, prompting the user to determine whether to quit the application that is not conforming to the behavior profile.

20

**EXPRESS MAIL LABEL NO.: EV343426261US**

21. A computer system for detecting intrusions, comprising:

a first memory for storing an application;

a second memory for storing a behavior profile associated with the application;

5 a monitor, communicatively coupled with the first memory and the second memory, for monitoring execution of the application, according to the behavior profile;

a warning module, communicatively coupled with the monitor, for issuing a message indicating that the application is not conforming to the behavior profile.

10

22. The computer system of claim 21, wherein the behavior profile is predefined when stored in the second memory, and wherein the behavior profile is generated by at least one of:

a developer of software for the monitor;

15 a developer of the application; and

a third party developer.